# Anomaly Detection Through Behavior Signatures

## ISRCS Briefing

**10 Aug 2010**

**Brett Borghetti**

**Electrical and Computer Engineering Dept**

**Air Force Institute of Technology**

**Sponsor: AFRL / 711 HPW/RHXB**

# Overview

- Parent Project Objectives
- Relation to Resilient Controls
- Large Scale Anomaly Detection

# Parent Project: AFRL City Beat

## Hypotheses:

- Cities have a pattern of life that can be studied and modeled
- Anomalous behaviors have transactional signatures
- Behavior models can be used for high fidelity simulations

## Objective:

- Develop an automated system with direct and indirect sensing to aid a human in anticipating, discovering and tracking nefarious transactions

# Core Team Members

- **John Duselis, PhD – AFRL / RHXB**
- **Rik Warren, PhD – AFRL / RHXB**
- **Jeff Graley, M.S. – AFRL / RHXB**
- **Lt Col Brett Borghetti – AFIT / ENG**
- **Prof. James W. Davis – Ohio State Univ.**
- **Prof. Amit Sheth – Wright State Univ.**

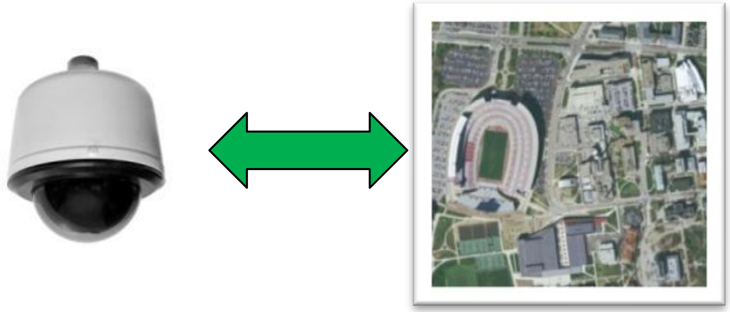
# Layers of Sensors & Data Types

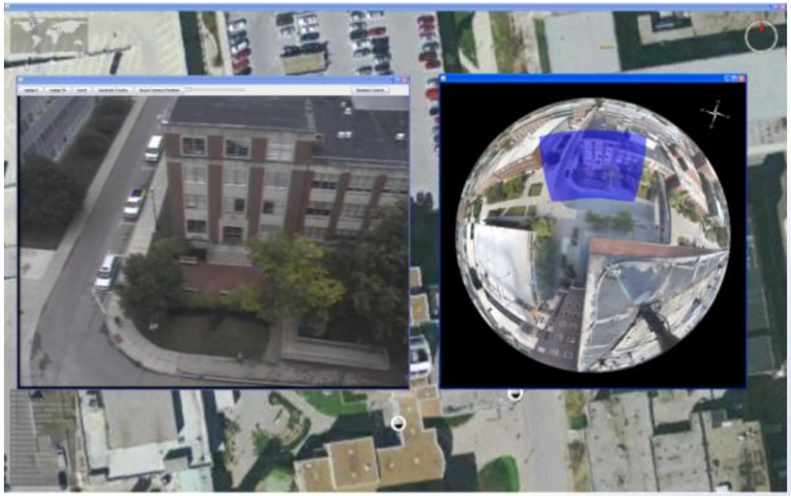
- Video cameras in public places
- Publically available web-based social networking data

# Interactive Visualization and Camera Control

**Matt Nedrich and Prof. James W. Davis**

**Ohio State University**





- Cameras fused with their environment
- Fully geo-registered framework
    - Live – pano – ortho registration mapping
- Multiple control layers for efficient camera control
- Allows operators to concentrate on environment rather than cameras
- Embedded GIS information (e.g., floor plans, class schedules)
- Upgrade of camera network

# Behavior Analysis

**Kevin Streib and Prof. James W. Davis**

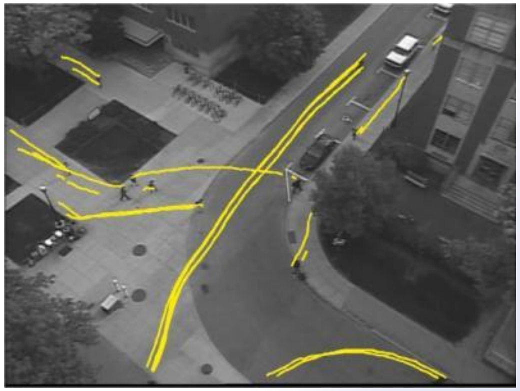
**Ohio State University**

**Objective:** Model the movement patterns of pedestrians and detect anomalies from learned behavioral trends.

**Research Tasks:**

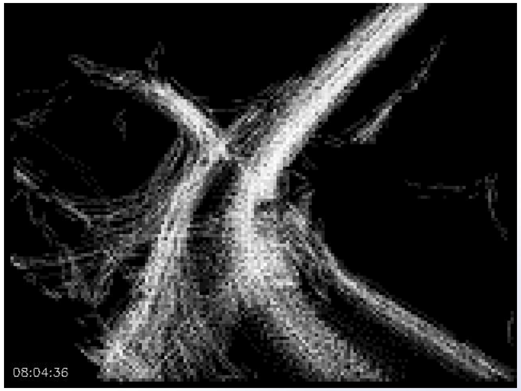
- Real-time multi-object tracking algorithm
- Accumulate tracks over time ( 24/7 )
- Search for "Patterns of Life" – Multiple Instance Learning
- Investigate influence of contextual factors
  - Day/Night, weather, scene density

Real-time Multi-object Tracking



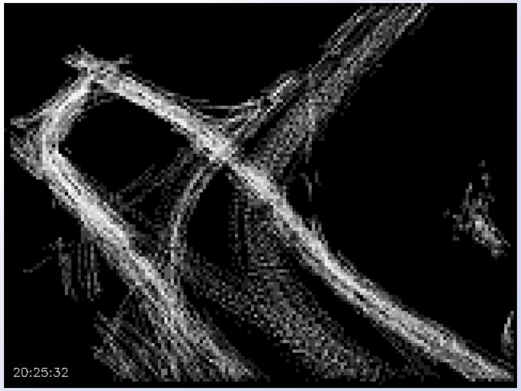
**Typical scene**

**Accumulated Tracks**



**Morning (8 am)**

**Accumulated Tracks**



**Evening (8 pm)**

# Example Scenarios

## Drop Off

-Drop off of person A and big bag

-Phone call made to person B

-Loitering of person A

## Bag Exchange

-Meeting

-Set down both bags

-Check for contents

-Walk off briskly

## Tracking of Bag

- Camera follows person B

-Person B walks towards bus stop

## Sensor Handoff

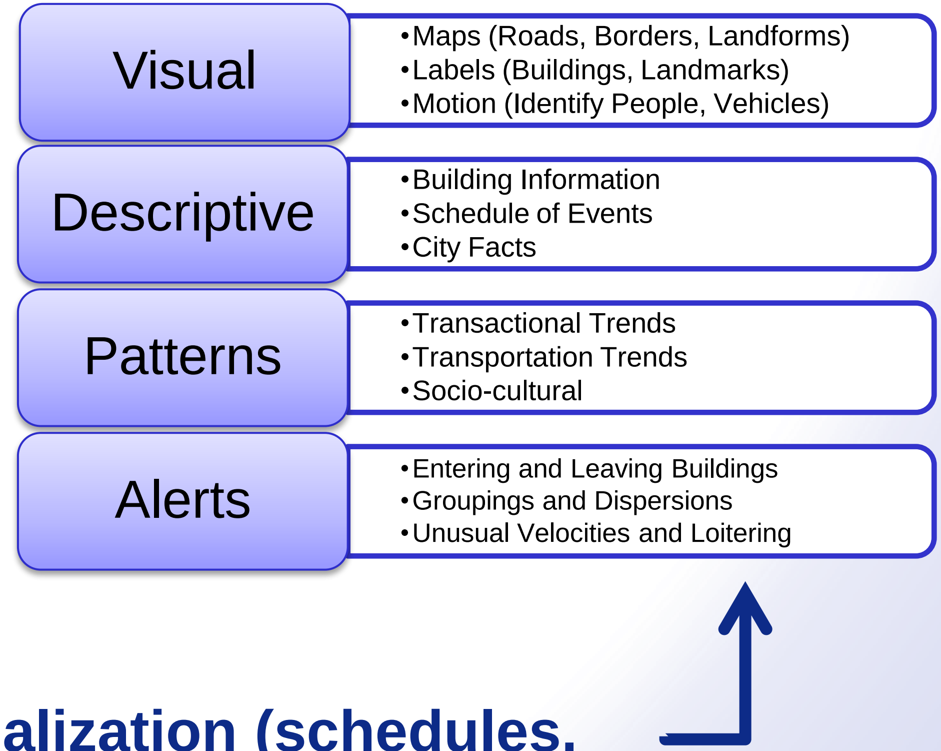
-Use bus system routes and schedule

-Follow bus, check for dismount using bus stop surveillance

# Experimentation Plans

- ➢Variety of alerts
  - ○ Unusual groupings
  - ○ Exchanges
  - ○ Unusual velocities/loitering
  - ○ Off the path

- ➢Confuser Events
  - ○ Buses group for orientation
  - ○ Textbook Hand-off
  - ○ Truck on sidewalk for construction



Visual
- •Maps (Roads, Borders, Landforms)
- •Labels (Buildings, Landmarks)
- •Motion (Identify People, Vehicles)

Descriptive
- •Building Information
- •Schedule of Events
- •City Facts

Patterns
- •Transactional Trends
- •Transportation Trends
- •Socio-cultural

Alerts
- •Entering and Leaving Buildings
- •Groupings and Dispersions
- •Unusual Velocities and Loitering

- ➢Prioritize and address alerts
- ➢Access indirect layers & visualization (schedules, maps, etc)
- ➢Ability to view multiple windows & multiple cameras simultaneously
- ➢Tracking capabilities
- ➢Histograms show patterns

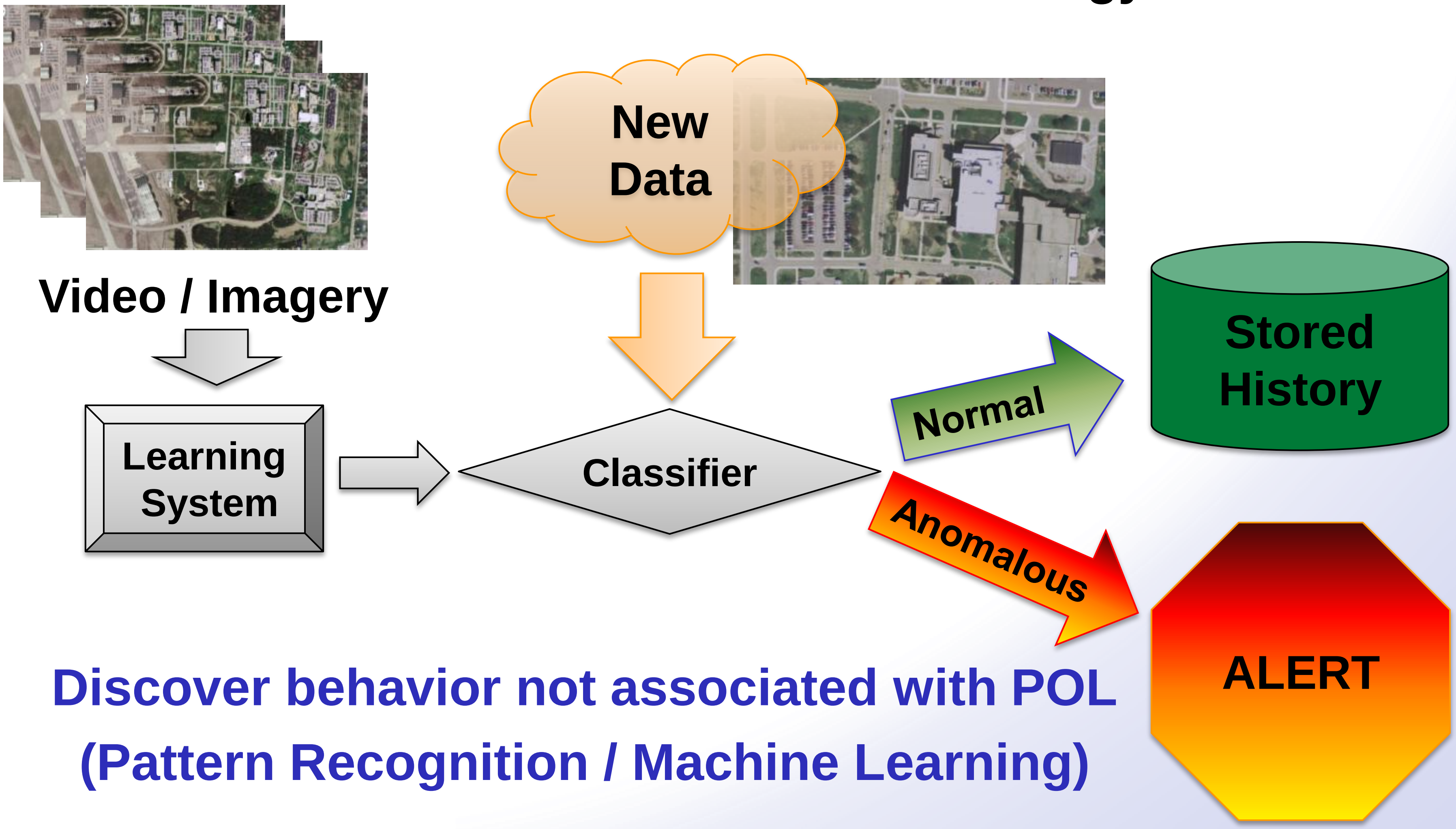
# Relationship to Resilient Controls

- **Goal: Increase situation awareness and security through video-based surveillance**
- **Assumption: Ever-increasing video availability, but human resources limited**
- **Problem: Too much video for unassisted humans to be fully effective in finding indicators & analyzing events**
- **Solution: Machine-aided anomaly detection and analysis**

# Large Scale Anomaly Detection

Lt Col Brett Borghetti

Air Force Institute of Technology

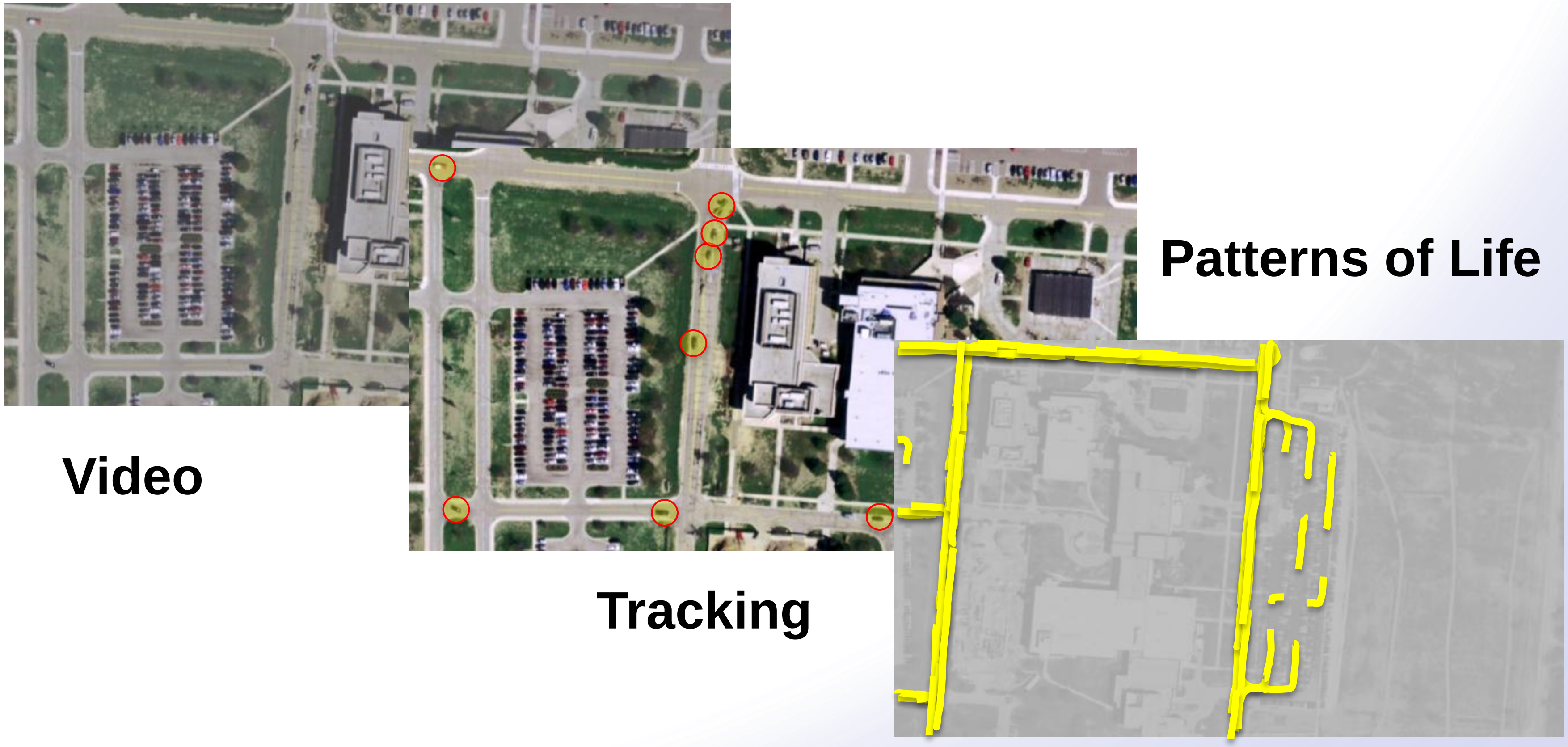


Discover behavior not associated with POL

(Pattern Recognition / Machine Learning)

# Building Patterns of Life Info

- Process Video
- Identify entities & tracks
- Aggregate POL from “normal” paths



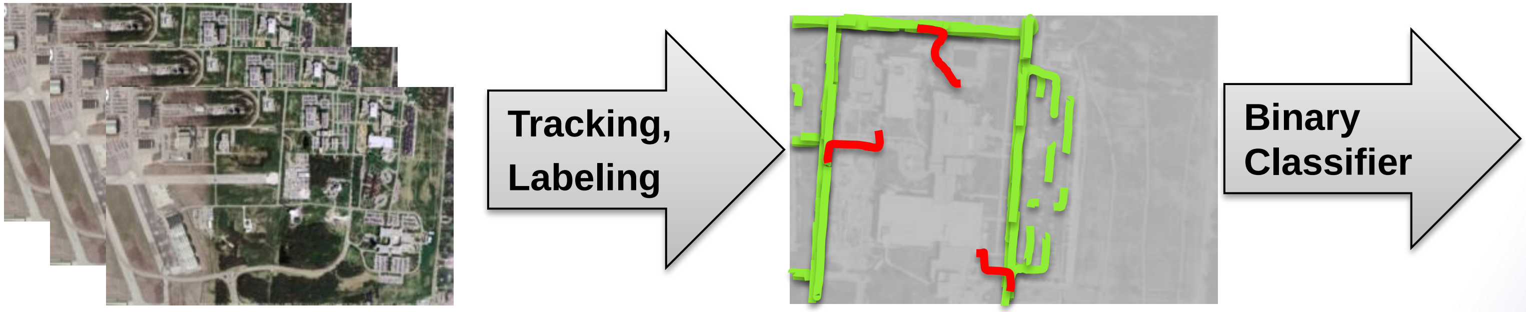
Patterns of Life

Video

Tracking

# Classifiers

Supervised



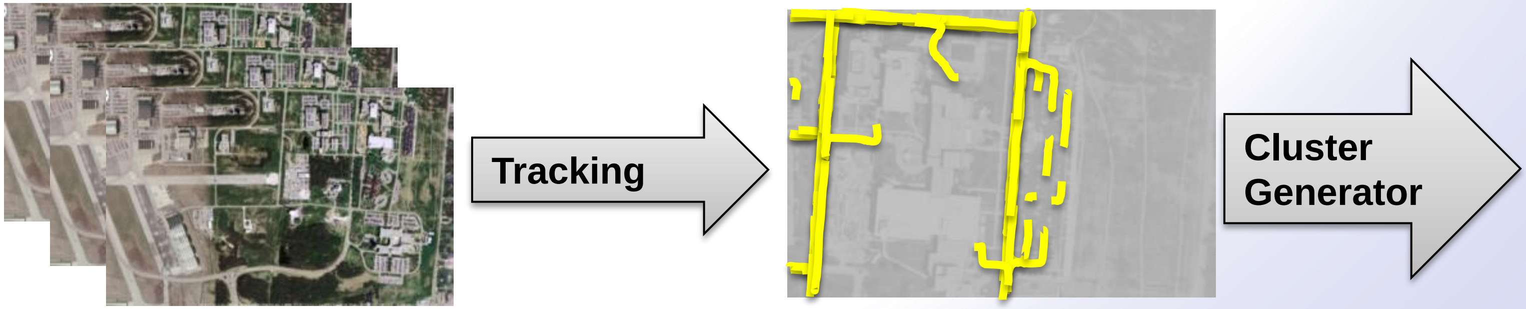
Tracking, Labeling

Binary Classifier

Video / Imagery

Labeled Track-space Data

Unsupervised (Clustering)



Tracking

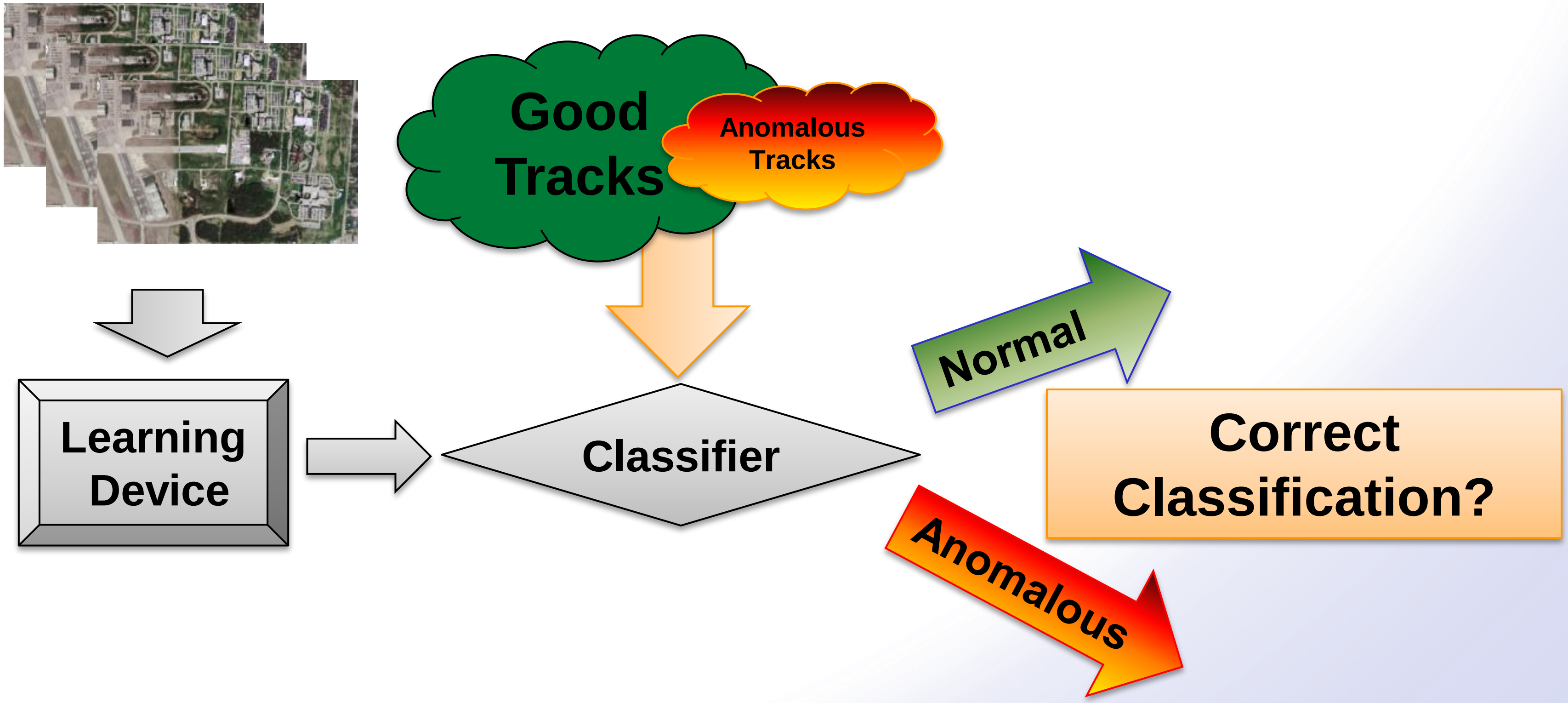
Cluster Generator

Video / Imagery

Track-space Data

# Validation with Anomalous Tracks

- Simplest method for initial testing of the classifier
- Hard to Visualize / Analyze the results
- Doesn’t evaluate image processing or tracker



# Challenges

- Need to validate *system* behavior
- Difficult / Expensive to coordinate anomalies during live collection
- Can we synthesize anomalous behavior?
  - Alter Image Data
  - Simulate Collection Process

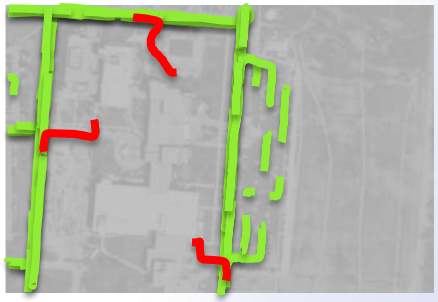
# Spiral 2: Image Manipulation

- **Alter images prior to tracking (or labeling)**
  - **Add entities that are behaving anomalously in each image**
  - **Use MATLAB to automate the process**

**Original**
**Video / Imagery**

**Add Anomalies**

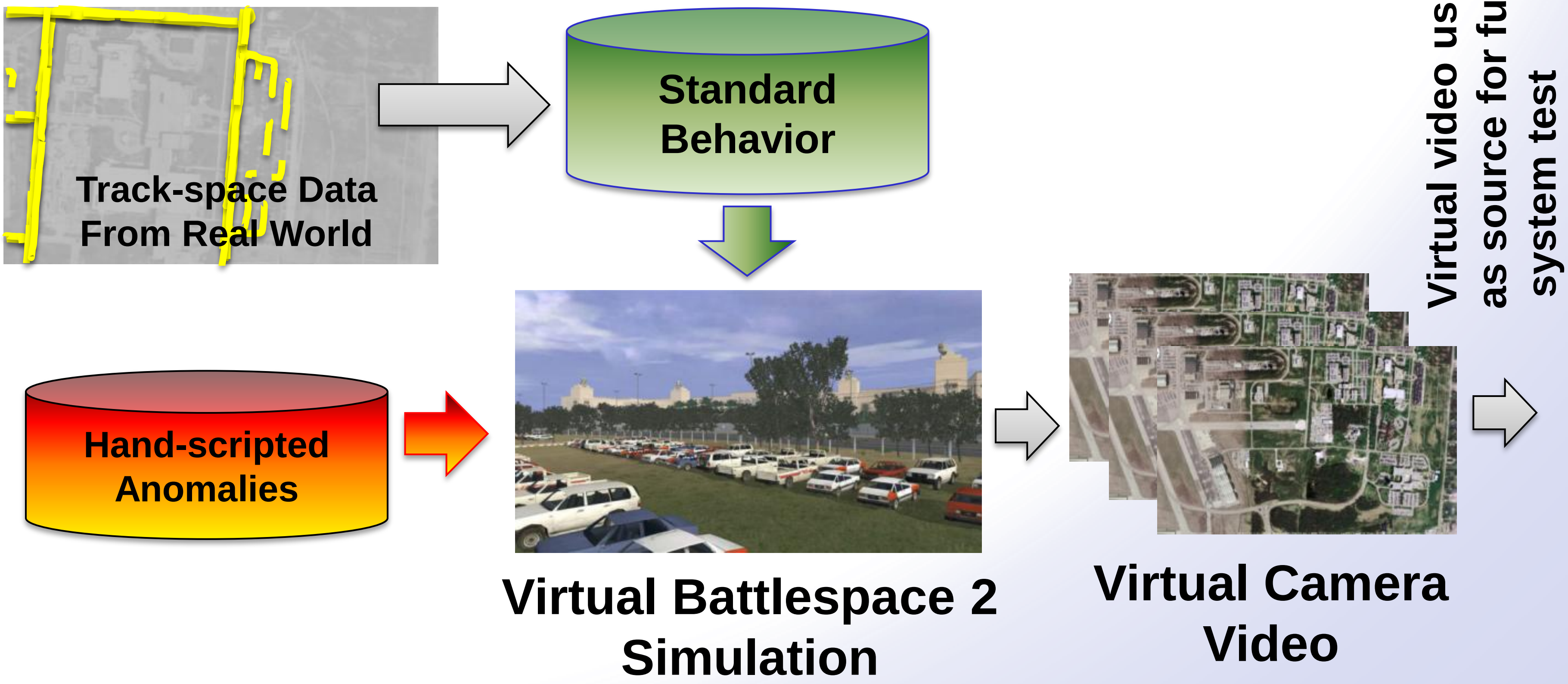
**Tracking,**
**(Labeling)**



**(Labeled)**
**Track-space Data**

# Spiral 3: Simulating Collection

- Recreate normal and add anomalous behavior within a simulated version of area of interest
- Collect & process video from simulation’s virtual camera to test end-to-end system



Track-space Data From Real World

Standard Behavior

Hand-scripted Anomalies

Virtual Battlespace 2 Simulation

Virtual Camera Video

Virtual video used as source for full system test

# Possible Future Work

- Compare performance of classifier with humans
- Model the human security worker’s actions
  - Decision to look for more info in existing data
  - Decision to take control of camera control / collection assets
  - Decision to direct emergency services / forces to anomalies